(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2002 (24.01.2002)

PCT

(10) International Publication Number
WO 02/06933 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/22463

(22) International Filing Date: 17 July 2001 (17.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/219,213 18 July 2000 (18.07.2000) US

(71) Applicant: **TOUCHSAFE.COM** [US/US]; Suite 201, 806 Governors Drive, Huntsville, AL 35801 (US).

(72) Inventor: **COCKERHAM, John, M.**; 2001 Colice Road, Huntsville, AL 35801 (US).

(74) Agents: **ROBERTS, Jon, L.** et al.; Roberts Abokhair & Mardula, LLC, Suite 1000, 11800 Sunrise Valley Drive, Reston, VA 20191 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/06933 A2

(54) Title: A SYSTEM AND METHOD OF MAKING ON-LINE PURCHASES WITH ENHANCED SECURITY

(57) Abstract: The present invention is a system and method of providing user PC-controlled encryption protocol. A merchant and a user are connected to a network. The user purchases items from the merchant with the transaction being processed through a credit card clearinghouse. Merchant provides a Book Mark Index and a Transaction Number to connected nodes. A User generates the encryption key by designating an encryption method and inserting the representative number at the Book Mark Index. The encryption key is sent to the Merchant and the Clearinghouse. The user sends the transaction number and associated information to a Clearinghouse. The user further sends shipping and communication data to the merchant and Data Pointers to the Clearinghouse. The user authenticates their person and the transaction, allowing the user to communicate with the Clearinghouse. The clearinghouse verifies the data pointers with the full customer profile. The Clearinghouse then verifies the customer's account balances and provides the transaction approval / disapproval directly to the Merchant. A Data Transaction Monitor tracks and pays the payment service for each approved transaction placed by a registered user.

Title: A System and Method of Making On-Line Purchases with Enhanced Security

Inventor: John M. Cockerham

Field of the Invention

1. This invention relates generally to purchasing of goods and services and other transactions via on-line transactions. More particularly, the present invention is a system and method of making purchases on-line with enhanced security for purchaser information.

Background of the Invention

2. Information transmitted over a computer network, including information relating to purchasing, can be easily accessed by many parties besides the intended recipient. For this reason, several methods of protecting the security of information transmitted over a network have been developed. Among them are Public/Private Key systems, symmetric key systems, and other security means. However, one of the problems associated with symmetric key systems is that the parties to the exchange must securely exchange the key. This may or may not be practiced for online transactions.

3. As part of any transaction online, credit card clearinghouses verify that the buyer has proper credit to pay the seller. Without the verification, the seller would not enter the transaction because he has no assurance that he will get paid. When transactions are conducted on line, the buyer, seller, and clearinghouse all must participate in the exchange of information. The problem with such transactions is that the buyer's personal financial information is transmitted over a network and potentially accessible to unauthorized parties. Though encryption methods are used to protect the user, they are primarily under merchant control. Thus the user has a problem because he cannot restrict the information available to the merchant.

4. One known system that operates a merchant control architecture is described in U.S. Patent No. 6,092,053 to Boesch, et al. for a system and method of merchant invoked electronic commerce. This patent discloses a system where the consumer's transaction information is stored on a Consumer Information Server. To complete a purchase transaction, the merchant collects purchase information about the consumer from the Consumer Information Server. The consumer has no approval or disclosure control once the transaction is submitted. Further, this system does not provide the consumer with a method of approving transactions of a named user of the account.

5. Another known on-line transaction service using bioidentifiers is provided by CHECKagain, Inc of Herndon, Virginia. The CHECKagain system allows a user to authenticate or approve on-line transactions using a bio-identifier. A user first registers his transaction information and registration information for all authorized users with the CHECKagain server. The user must register at a CHECKagain facility or kiosk. If the user or another user of the account makes a transaction, the user can approve the transaction by submitting his bioidentifier to the CHECKagain server. For the approval to take place, the bioidentifier information is transmitted over a network and compared to the bioidentifier on file for matching results. Thus, the user's identifying and personal information is transmitted over the network. As a result, the user's confidential information is not within the user's control and is subject to the vagaries of Internet transition.

6. Encryption systems are used primarily to protect the confidentiality of the information being transmitted. However, due to the nature of data transmission over a network, encryption systems must serve additional purposes. Encryption systems have an authentication function. Authentication allows the receiver to verify the origin of the message, and ensure no

transmission by an imposter occurs. Encryption systems can determine message integrity. Integrity allows the recipient to know that data has not been changed during transmission, from partial dropouts to a completely false message. Encryption systems additionally provide nonrepudiation guarantees. Nonrepudiation techniques prove that a sender did send a transmission and prevents the sender from denying that he is the source of a transmission.

7. Current systems for online purchasing put control of personal information and privacy with the merchant in a transaction. Encryption is used to protect transmitted information. Since the merchant controls the transaction format, the merchant also has control of the customer's personal information. Thus, the user is not in control of protecting himself and his private information. What is needed is a system and method of secure purchasing that has personal information verification that is controlled by the user.

Summary of the Invention

8. It is therefore an objective of the present invention to provide a system and method of secure financial data transfer.

9. It is a further objective of the present invention to allow a user to control the amount of personal information transmitted over the Internet.

10. It is another objective of the present invention to separate the locations of where user identification and transaction validation are performed.

11. It is yet another objective of the present invention to allow a user to designate a method of encryption at the user's computer.

12. It is a further objective of the present invention to allow a user to authenticate a transaction with a bio-identifier.

13. It is still another objective of the present invention to allow a customer to provide transaction identification data at a user computer versus at a remote server.

14. It is a further objective of the present invention to provide an encryption key protocol to multiple nodes necessary to a transaction.

15. It is still another objective of the present invention to restrict transaction information available to a merchant to only a transaction number and to exclude the customer's credit card information.

16. It is still another objective of the present invention to allow a user to provide bio-authentication information to authorize the user's on-line transaction.

17. It is still another objective of the present invention to relieve the merchant of primary responsibility for maintaining on-line transaction security.

18. It is yet another objective of the present invention to prevent unauthorized users of a credit card to complete a transaction.

19. It is another objective of the present invention to reduce the time needed for an on-line transaction.

20. It is a further objective of the present invention to provide data pointers, and not full data information, needed to complete a transaction.

21. It is still another objective of the present invention to make transaction data meaningless to an interceptor.

22. The present invention is a user controlled encryption system and method useful for conducting financial or purchase transactions (collectively "transactions") on-line in a secure fashion. A merchant, user, and clearinghouse are connected to a network which is preferably, but without limitation, the Internet. Other networks used for purchase transactions are also

suitable for the present invention. The user purchases items from the merchant with the transaction being processed through a credit card clearinghouse. Both the user's computer and the clearinghouse have a number of pre stored encryption methodologies. Each methodology is identified by a number or other ID (encryption ID). The clearinghouse already has complete user information in the form of user credit information. The merchant provides a Book Mark Index and a Transaction Number to track the user transaction to connected nodes. The user generates an encryption key and designates an encryption method (represented by the encryption ID) and inserts the encryption ID at the Book Mark Index. The user sends the transaction number and data field pointers to the Clearinghouse in encrypted form. The user further authenticates the transaction by providing a bioidentifier at the user's computer. The users computer comprises software for recording and recognizing the user's selected bioidentifier. If the bioidentifier is authenticated, the user is permitted to complete the transaction. The encryption key, generated by the user's PC, along with the encryption ID is sent to the Clearinghouse and the merchant. The Clearinghouse then decrypts the message and identifies full user information indicated by data pointers. If the user then has sufficient credit available, the Clearinghouse so notifies the merchant by sending an encrypted message to the merchant, providing an authorization, and identifying to the merchant the transaction that is authorized via the transaction number. A Data Transaction Monitor tracks and pays the payment service for each approved transaction placed by a registered user.

Brief Description of the Drawings

Figure 1 illustrates the architecture of the present invention. According to one embodiment

Figure 2 illustrates the process flow of the present invention. According to one embodiment

Detailed Description of the Invention

23. The present invention is a system and method of providing secure transactions over a network with a user-controlled encryption and data security. Referring to **Figure 1**, the architecture of the present invention is illustrated. A merchant computer **10**, a user computer **20**, a clearinghouse computer **40**, and a data transaction computer **50** are connected to a network **5**. Typical personal computers having a processor and memory known in the art are used to practice the present invention. A Pentium processor having 16 MB or higher of memory supports the present system. Additionally, computers **10, 20, 40, 50,** have Internet access capability. Modem, fiber, or any other network connection known in the art can support the architecture of the present invention. The network **5** is preferably the Internet although this is not meant as a limitation. Other private and public networks are also suitable for transactions of the present invention.

24. The merchant computer **10** stores and executes software for processing transactions over the network **5**, including the necessary encryption and decryption software and data. The merchant computer **10** generates and assigns a random number Book Mark Index **12** for each transaction. The merchant computer **10** also generates a transaction number **14** for each transaction. The merchant computer **10** stores any purchase information in a purchase information database **16**. Purchase information is any information other than the user's credit card number, such as the user's shipping address, which does not violate the user's privacy when transmitted over a network in an unencrypted form.

25. User computer **20** of the present invention comprises software for generating an encryption method to be randomly selected from several different methods **22**. When an encryption algorithym is selected, it is identifies by an encryption method ID (encryption ID). The user computer **20** comprises a customer database **24**, a bioidentifier device **26**, and a communications log database **28**. The encryption method generation **22** associates encryption methods with random number identifiers generated by the User PC **20**. The customer identification database **24** contains a user's purchase information, such as name, address, credit card number, authorized user names, and any other information needed to complete a transaction. A bioidentifier device **26** is connected to the user computer **20** and is used to identify a current computer operator. Bioidentification data is stored in the customer database **24**. Bioidentifier devices use a biological trait of a person to identify them as a party to on-line activities. A common such device on the market today is the fingerprint identifier. Fingerprint identifiers, compatible with a personal computer, are available from technology manufacturers such as Link-It Technologies, or Cross-Match Technologies. Although a fingerprint identifier is preferred, it is not meant as a limitation. Other bioidentification systems can be used, including but not limited to retinal scanners, voice recognition systems, and palm print systems. The user computer **20** further includes a communications log database **28** for recording all transmissions made from the user computer **20** for on-line transactions. If there are any transaction discrepancies, the communications log database **28** is used to determine what occurred between parties to a transaction.

26. The system of the present invention includes a clearinghouse computer 40 with the necessary encryption and decryption software. With algoritheims that match those of the user computers inventory of encryption methods **22**. The clearinghouse computer **40** includes a

customer database 42, a merchant database 44, and a communications log database 46. The customer database 42 stores information files for each having a credit card or other credit record that is maintained by the clearinghouse. The information files include information needed to authorize and complete a transaction, including customer names, addresses, credit card numbers, authorized users, and the like. The merchant database 44 contains all participating merchant information as well as transaction protocols preferred by each merchant. The communications log database 46 records all transmissions made from merchant and user computers. The Clearinghouse computer also comprises software for receiving the encrypted transaction information from the user computer, a decryption database having the same algorithms as the user computer for decrypting with associated encryption ID's the transaction information for identifying the user via pointers in the transaction information, and for authorizing the transaction in the normal fashion.

27. The system of the present invention comprises a data transaction computer 50. The data transaction computer tracks information for the system administrator. The Data transaction computer 50 includes a registered customer database 52 and an approved transactions database 54. The registered customer database 52 stores a customer identification for each user of the purchase service. The approved transactions database 54 stores the transaction number of all transactions placed by registered users and approved by a clearinghouse used by the purchasing service. Although disclosed as separate, the data transaction computer 50 can also be incorporated into the clearinghouse computer system.

28. A user views merchant web pages on the user computer 20. Using known Internet protocols, the user browses web pages to view items for sale. In this manner, the user can decide whether he wishes to place an on-line transaction.

29. Referring to **Figure 2**, the process flow according to one embodiment of the present invention is shown. A user desires to make on-line purchases. The user also desires to make on-line purchases while keeping his personal information secure. The user registers with software on the user's computer **100**. During registration, the user provides the user software with all identification information. This information remains resident on the user computer. The user provides credit card numbers, authorized user names, his billing address, his shipping address, bioidentifiers and all other information required in a commercial transaction. All authorized credit card users log in to the user computer by providing, such as by scanning in, their respective bioidentifiers. For instance, where the bioidentifier is a fingerprint, the user will place his finger on the scanner connected to his user computer. The fingerprint is then compared to the stored fingerprint at the user's computer. If a favorable comparison is made, the user is allowed to continue with the transaction. Without the authentication, the user computer cannot forward any information to the clearinghouse computer. Using this authentication process is particularly advantageous for preventing credit card fraud. No transaction will take place without the proper authentication. Additionally, any thief would need to leave behind a fingerprint, and is thus deterred from using the credit card.

30. The user further submits registration information to the clearinghouse computer **105**. By using the software of the present invention, the user's information is encrypted when sent to the clearinghouse. Further, associating the user with a credit card number only happens during one on-line transmission instead of happening every time the user makes an on-line transaction. Advantageously, this significantly reduces the amount of times a user's information is susceptible to interception and in a form that is meaningful to the intercepting party. In order to increase security, the user may provide the registration information to the clearinghouse

computer by United States mail. The user's information is then entered into the registration database via computer internal to the clearinghouse network. In this respect, the user is never associated with a credit card number during an on-line transmission of information. Further, the user's credit card information is never provided to the merchant. Advantageously, the user's credit card number cannot be stolen by any unauthorized access of the merchant computer.

31. From this point onward, only the user whose bioidentifier has been associated with the personal information can access that information to consummate a transaction. The software then identifies the user as being registered with the payment system. The user's registration is stored in the registration database of the data transaction computer.

32. Subsequent to registering, the user desires to place an on-line transaction. The user selects items via a shopping cart web page maintained by the merchant. When the user has compiled his list of desired items, he transmits the request for purchase to the merchant **110**. The request for purchase includes an indication that the user desires to use the system of the present invention. The user indicates using the system by selecting an icon. The icon can be present on the user's computer, the merchant's web page, or both. The request for purchase may additionally includes transmitting the user's shipping address from the customer identification database **24** (shown in figure 1). The merchant uses the shipping address information to calculate appropriate shipping costs for the order. However, it is also contemplated that the software of the present invention includes the user's shipping address in the encrypted message as further described below.

33. The merchant computer assigns a Book Mark Index and a Transaction Number specific to the transaction. The Book Mark Index is a randomly generated number designating a location for the encryption key. The merchant computer stores and sends the Book Mark Index and the

Transaction Number, the price and identity of goods to the user computer 112 and the clearinghouse computer **112**.

34. Upon receiving the Book Mark Index, goods description, price, and Transaction Number, the clearinghouse computer opens a transaction. The user computer generates an encryption key. To generate an encryption key, the user computer must generate both an Encrypt Key and a Sequence Number. The Encrypt Key is a random positive integer from one to five (for example). Each number is assigned to a specific encryption method. Next the user computer generates a Sequence Number. The Sequence Number is a random number of 99 characters. The Sequence Number includes the Encrypt Key Number. The Sequence number is then inserted in the proper character position designated by the Book Mark Index.

35. The user computer further creates Data Pointers. Data Pointers are partial bits of the user's personal information which would not identify the user to a credit card if intercepted. One example of a Data Pointer is the last four digits of a credit card account. Another Data Pointer might be the user's initials. The Data Pointer is primarily designed not to identify any specific person if the transmission of the data pointer were intercepted and read by an unauthorized party. The full Sequence Number containing the Encrypt Key Number and the Transaction number are transmitted to the merchant computer **114**. The user next authenticates the transaction at the user computer **118**. In the preferred embodiment, the user authenticates the transaction by entering his bioidentifier. The user PC compares the bioidentifier given for the transaction to the bioidentifiers provided during registration with the user PC, as previously described in step **100**. If authentication is successful, the user computer is free to continue processing the transaction.

36. As noted above, the merchant computer sent a transaction number to the user **112** for use by the user and for subsequent transmission by the user to the clearinghouse computer. The user

authenticates himself with his bioidentifier, permitting the user PC to then send the Sequence Number, encrypt key number, Transaction Number and transaction information and Data Pointers to the clearinghouse computer **122**.

37. The clearinghouse computer receives and decrypts the transaction information, i.e.- the transaction number and price, according to the identified algorithm. The decrypted transaction information and data pointers submitted by the user is matched with the customer profile. The clearinghouse computer cross references the data fields against the full user profile. If the information matches, the clearinghouse knows the transaction is entered by the registered user and is authentic. The clearinghouse further verifies that the user has sufficient credit to support the transaction. If all the information is correct and approved, the clearinghouse computer enters the transaction. The merchant is notified, preferably in encrypted form, that the transaction is approved strictly by receiving the approval and the transaction number **128**. Thus, the transaction has been entered, yet no personal identification of the user, particularly being associated with a credit card number, has ever been transmitted to the merchant.

38. The clearinghouse computer sends a notification message to the data transaction computer **130**. The data transaction computer stores the transaction number of each approved transaction. The system provider is paid according to the number of transactions placed. Since the clearinghouse has authority to charge to the user's credit card, the clearinghouse can immediately enter service payment for the transaction. For instance, the clearinghouse computer could send ten cents per approved transaction to the data transaction computer. Similarly, any other terms of service agreed to between the parties could be used. The users registration number is also part of the notification message. The registration number lets the system provider

know where to send account information, such as special promotions, software upgrades or provide other marketing or customer service services to the user.

39. The user enjoys particular security in knowing that the transaction occurs without any transmission of information which can identify the user if intercepted. Further, the user's trust when placing on-line transactions is developed without any cost to the merchant. The security encourages users to buy more frequently in two respects. First, purchases occur more quickly because the user does not need to repeatedly enter identification information. Thus, the user can buy more and is more likely to purchase impulsively. The user also becomes comfortable with placing on-line transactions because all the transactions occur in the same manner regardless of the merchant used.

40. The merchant and credit card companies also benefits from the increased transactions. Both see larger sales volume without expense. Further, the merchant and the credit card company actually have reduced manpower, service, and system use because the system provider reduces the information processing burden.

41. An additional benefit is realized for users because the bioidentifier information is stored in the customer identification database **24** (shown in Figure 1). This information may serve to aid law enforcement in identifying missing children or other persons if the user allows the information to be divulged for these purposes.

42. Although the system and method of the present invention has been described with several information fields transmitted at one time, it will be appreciated by those skilled in the art that information fields may be transmitted separately.

43. A system and method of user-controlled encryption protocol has been described. It is obvious to one skilled in the art that a wide variety of web-enabled devices adapted for use with

bioidentifiers, such as mobile phones, PDA's, or web phones with a bioidentifier means, may be used without departing from the scope of present invention as disclosed.

We claim:

1. A system for conducting on-line transactions with enhanced security over a network comprising:

a user computer, the user computer further comprising a bioidentifier peripheral, a processor and memory,

wherein a bioidentifier of a user is stored in the user computer memory;

a clearinghouse computer;

a data transaction computer; and

a merchant computer;

wherein the user computer, the clearinghouse computer, the data transaction computer, and the merchant computer are connected to the network; and

wherein the user computer further comprises logic for permitting the user to enter a bioidentifier into the user computer using the bioidentifier peripheral, for comparing the entered bioidentifier with the stored bioidentifier and for requesting the clearinghouse computer to enter a transaction only if the entered bioidentifier is the same as the stored bioidentifier.

2. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the network is the Internet.

3. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the network is a wireless network.

4. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the network is an intranet.

5. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the bioidentifier is a fingerprint scanner.
6. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the bioidentifier peripheral is a face print scanner.
7. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the bioidentifier peripheral is a retinal scanner.
8. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the bioidentifier peripheral is a palm print scanner.
9. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the bioidentifier peripheral is a voice print scanner.
10. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the transaction is a purchase of goods or services.
11. The system for conducting on-line transactions with enhanced security over a network of claim 1 wherein the transaction is an access and distribution of information.
12. A system for providing enhanced security for on-line transactions conducted over a network comprising:

a user computer having a processor and a memory connected to a network, the user computer further comprising:

a bioscaner;

a customer database comprising customer data stored in the user computer memory;

a plurality of encryption logic stored in the user computer memory and

instructions for randomly selecting one of the plurality of encryption logics and for encrypting transaction information according to the randomly selected encryption logic; and instructions for creating data pointers from the customer data;

a clearinghouse computer having a processor and a memory connected to the network, the clearinghouse computer further comprising:

a customer database stored in the clearinghouse computer memory;

a merchant database stored in the clearinghouse computer memory;

a communications log database stored in the clearinghouse computer memory;

wherein the clearinghouse computer further comprises instructions for encrypting and decrypting transaction information according to the randomly selected encryption logic assigned by the user computer;

a data transaction computer connected to the network; and

a merchant computer connected to the network;

wherein the user sends a transaction request to the merchant computer over the network, the merchant computer generates a book mark index and sequence number, the merchant computer transmits the book mark index and sequence number to the user computer over the network, the user computer generates an encryption key and encodes the transaction information, according to the randomly selected encryption logic.

13. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the network is the Internet.

14. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the network is a wireless network.

15. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the network is an intranet.

16. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the bioscanner is a fingerprint scanner.

17. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the bioscanner is a face print scanner.

18. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the bioscanner is a retinal scanner.

19. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the bioscanner is a palm print scanner.

20. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the bioscanner is a voice print scanner.

21. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the transaction is a purchase of goods or services.

22. The system for providing enhanced security for on-line transactions conducted over a network of claim 12 wherein the transaction is the access and dissemination of information.

23. A method of providing enhanced security for an online transaction comprising:

a user sending a transaction request from a user computer to a merchant computer;

generating a book mark index and sequence number for the transaction at the merchant computer;

transmitting the book mark index and sequence number to the user computer;

randomly selecting an encryption method and placing an ID for the selected

encryption method in the sequence number at the user computer;

transmitting the book mark index, sequence number, and the ID, to a clearinghouse computer;

entering a bioidentifier of the user requesting the transaction into the user computer;

comparing the bioidentifier of the user to a customer database of authorized user bioidentifiers stored in the user computer;

sending an authorization to proceed from the user computer to the clearinghouse computer if the bioidentifier of a person requesting the purchase matches the authorized user bioidentifiers stored in the user computer;

selecting a set of data pointers from the customer database stored in the user computer and transmitting the set of data pointers to the clearinghouse computer;

verifying at the clearinghouse computer that the transaction has been approved by an authorized user and that the user has sufficient credit to support the transaction; and

notifying the merchant that the transaction is approved.

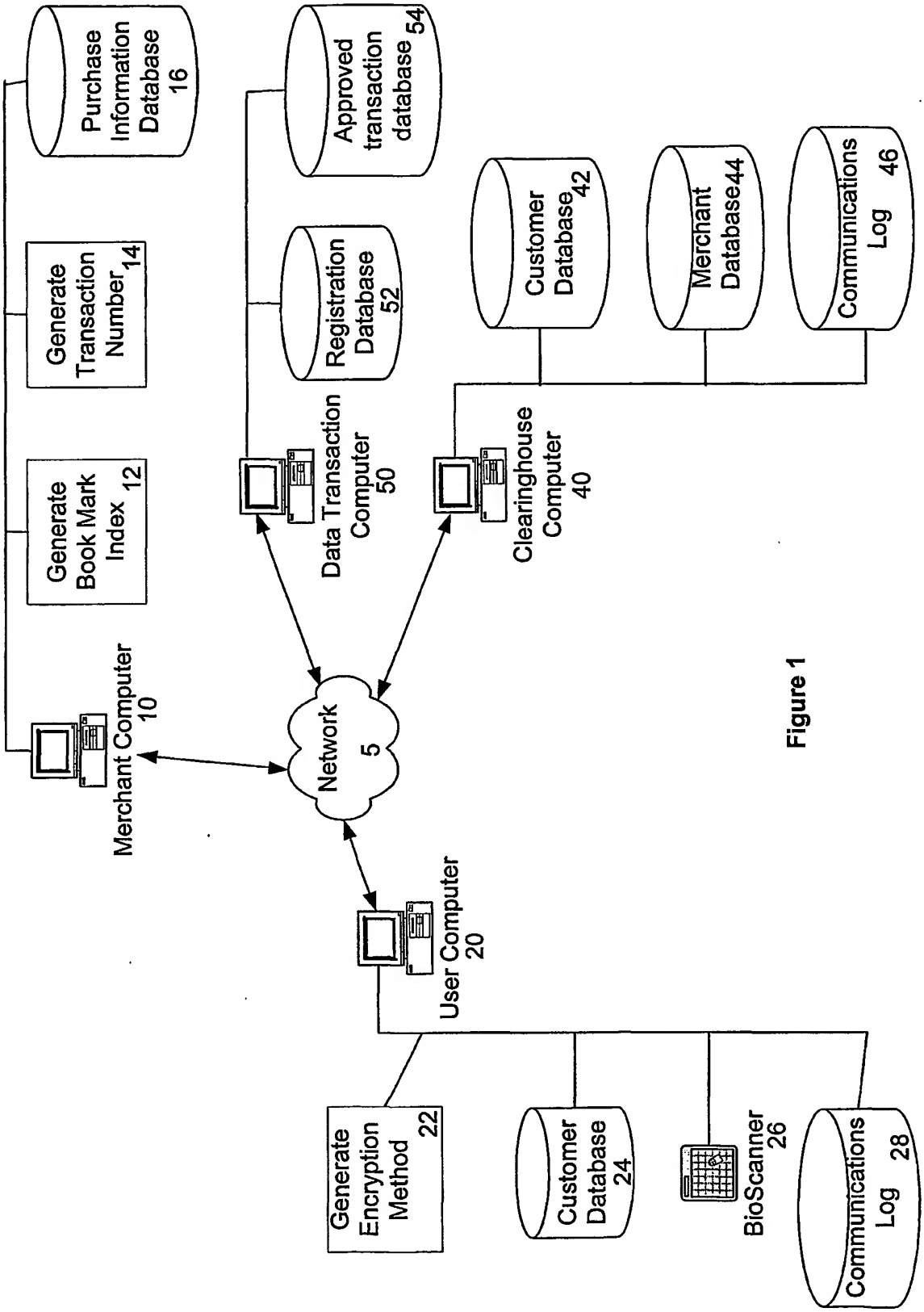
Purchase Information Database 16
Approved transaction database 54
Generate Transaction Number 14
Registration Database 52
Customer Database 42
Merchant Database 44
Communications Log 46
Generate Book Mark Index 12
Data Transaction Computer 50
Clearinghouse Computer 40
Merchant Computer 10
Network 5
User Computer 20
Generate Encryption Method 22
Customer Database 24
BioScanner 26
Communications Log 28

Figure 1

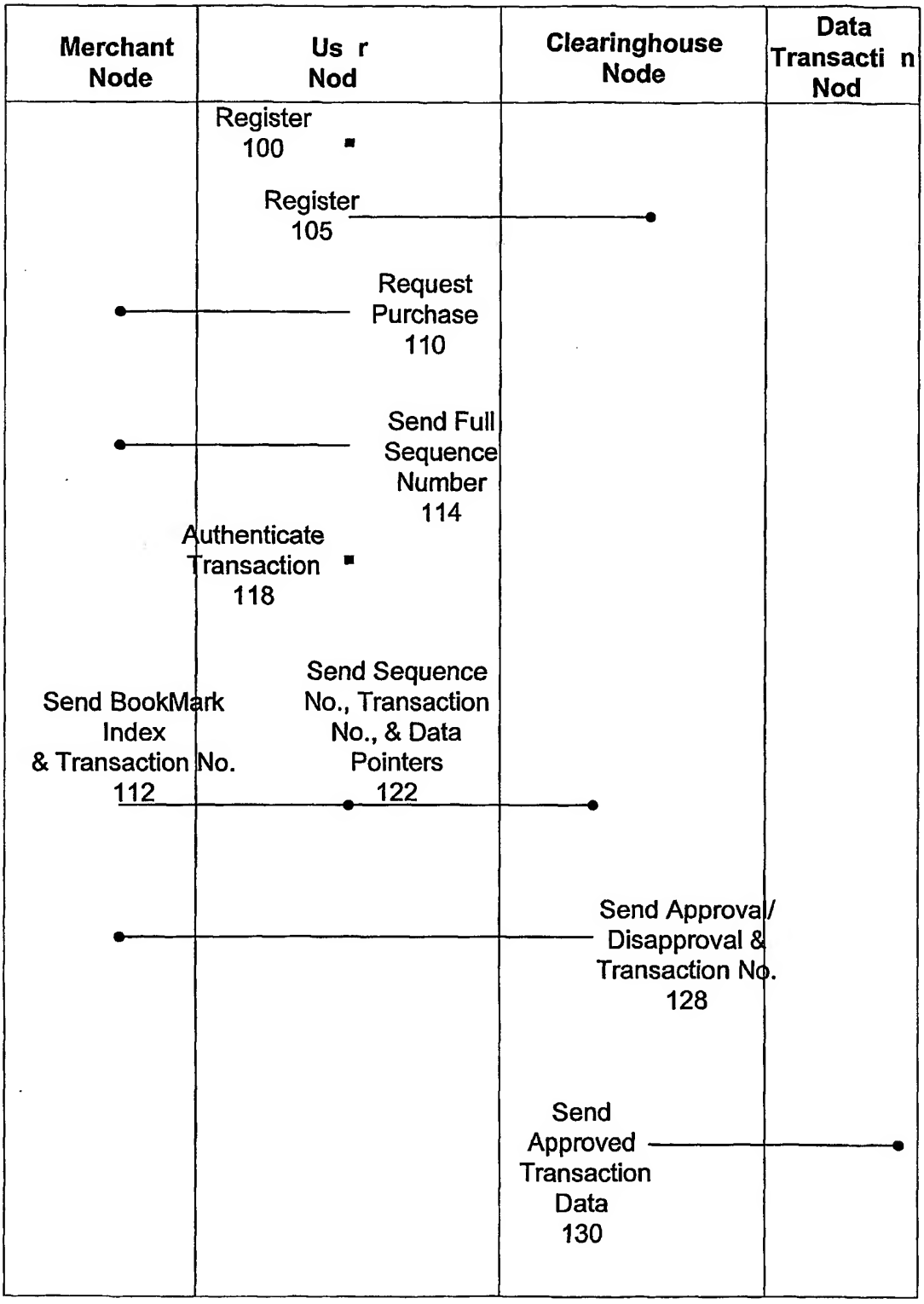
Merchant Node
Us r Nod
Clearinghouse Node
Data Transacti n Nod
Register 100
Register 105
Request Purchase 110
Send Full Sequence Number 114
Authenticate Transaction 118
Send BookMark Index & Transaction No. 112
Send Sequence No., Transaction No., & Data Pointers 122
Send Approval/ Disapproval & Transaction No. 128
Send Approved Transaction Data 130

Figure 2